Published and Copyright (c) 1999 - 2003
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Kevin Savetz
Jens Heitmann

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
http://www.icwhen.com/aone/
http://a1mag.atari.org
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ The Light of Adamas! ~ People Are Talking! ~ Doom III Delayed!
~ Do We Have Spam Apathy ~ SEC Probes Game Makers ~ Draconis News!
~ Tips to Avoid Scams! ~ New Anti-Spam Vendor! ~ Spammer Tricks!
~ New Web Scam: Phishing ~ Scamming the Scammers! ~ New WriteATR Version

-* Online Voting Nears Reality! *-
-* Web Scams Linked to Identity Theft! *-
-* Do Not Spam Registry Finds Favor in Senate *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, let's see. If the weather this past week was mostly thunderstorms and rain, I must have been on vacation! It almost never fails. It's an ongoing joke at work! Oh well, there's nothing one can do about it. And, I still have another week to go. So far, the vacation has actually been quite nice.

I actually have a lot to say this week, but since my brain is on "mellow" this week, I won't really go at it. But, it appears quite obvious these past few weeks that the focus on computing news has been on the side of seedy topics. We've been deluged with news regarding spam, internet fraud, and illegal music-swapping. This "Information Super-Highway" has certainly been a wonderful trip! This is not new news - just taking a different twist of something we've been plagued with for years in one form or another. Will government regulation cure these ills? I doubt it, but we'll see.

Until next time...

=~=~=~=

Draconis News 9/2003

Draconis News 9/2003

* Draconis Driver for MagicPC v0.1

The first driver version for Draconis Programs running with MagicPC is now available. This offers a direct internet connection over the TCP/IP of Windows, which enables access over Ethernet, DSL and connections via Analog or ISDN modem (cards) also under MagicPC.

The driver is available at:

http://draconis.atari.org/draconis/archives/drac_mpc.zip

* The Light of Adamas

The current Adamas version is 1.8 Pre-Release 20.

The main changes are:

*** Adamas 1.9 Pre20 ***
- N.AES adaption
- Font dialogue GEM
- URL droplist GEM
- Autodrop GEM
- Image behaviour during download
- Download pauses optimized
- Memory was destroyed in Online mode (TITLE)
- Double memory freeing fixed.
- Online Access/Refresh
- ALL-Array now still correct after a refresh.
- URL input now handled by standard dialog handler.
- Slider overwrote Symbol
- Fix in download of small pages
- Slb-Fix.
- Anchor jump to an ID.

The Pre-Release is available at:

http://draconis.atari.org/draconis/archives/ada18dev.zip

a 68030 version is available at

http://draconis.atari.org/draconis/archives/ada18d30.zip

--
Jens Heitmann
http://draconis.atari.org
draconis@atari.org

Adamas 1.8 Pre-Release 22

Hello,

(7/24/2003)
Adamas 1.8 Pre-Release 22
http://draconis.atari.org

Pre-Release 20 is a Release-Candidate of the final version 1.8. Some improvements in the GEM implementation, beside some other changes. For installation you need an installed version 1.7, because the 1.8 files are only replacements or extensions to it.

(68000)
http://draconis.atari.org/draconis/archives/ada18dev.zip

(68030)
http://draconis.atari.org/draconis/archives/ada18d30.zip

Best regards,
Paul
Paul CAILLET.

New WriteAtr with Experimental Enhanced Density Support

I've uploaded a new version of WriteAtr (V0.92b) to my homepage

http://www.horus.com/~hias/atari/

This version contains experimental support for the enhanced density (1040 sectors in MFM) format.

Although most of my datasheets about uPD765 compatible floppy controllers contain a note that this format (128 bytes per sector in MFM) doesn't work, some experiments showed that my PC (350MHz P-II, ASUS P2B mainboard) is able to create this format, but it cannot read the disk it just wrote :-) But then - my stock 1050 happily read from and wrote to the disk!

So feel free to try it with your PC. I can't guarantee it will work at all for you so use it at your own risk!

BTW: for those of you who don't like to read manuals, here are the command line parameters to use the enhanced density format:

```
writeatr -f9 -n my.atr
```

so long,

Hias

=~=~=~=

PEOPLE ARE TALKING

compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. It's been a tough couple of weeks for me. I apologize for having to skip out on last week's column, but there was just no way I could do anything meaningful... or even intelligible.

My grandfather, who is 91 was hospitalized with pneumonia, has taken a lot of my time the past few weeks. It's amazing to me that doing little other than sitting in a chair and keeping someone company can be so draining. But draining it is.

Anyway, one of the subjects that my grandfather asks about often is how I'm able to communicate with relatives on the other side of the continent without incurring a huge charge. The fact that instant messaging is easy to do mystifies him, as does the fact that there's no charge for doing it like there is for long-distance telephone calls.

He just can't wrap his mind around the fact that you don't need any special knowledge or particularly unique equipment to send instant messages. In his day he was one of those guys who had a police scanner

and CB radio going all the time and knew just about everything there was to know about using them. That was years ago, though, and he hasn't used them in years. His hearing is now so bad that he can't understand anything that's being said.

I guess that's just the way things go... you get to a point where you're comfortable with what you're doing and you stop keeping up with technology. I've seen it over and over again with everything from small businesses to personal computers. People who bought a Coleco ADAM, a TI99-4A, or even an Atari ST, and then stopped keeping up with what was going on.

Personally, Atari computers will always have a very special meaning for me. I've owned a bunch of different computers from my first TimeX-Sinclair ZX81 to a Commodore64 to all my different Atari computers, Intel machines, and even a Macintosh.

But of all those machines, I must confess that computers running TOS were the only ones to make me feel comfortable. There was just something special about them. They had personality. They did the things I wanted to do, they let me do whatever it was easily, and it was actually fun to use them.

I'm much more productive with my spiffy Intel laptop, but it's just not as much fun. There's no personality to this machine. Sure, it's fast, it displays tons of colors, it's even "mainstream"... when I'm running a Microsoft OS on it instead of Linux... but it's not the same.

I have never claimed to be a computer wizard or to have any talent at programming whatsoever, and yet I was much more at home with a "less advanced" computer like the ST than this Intel-based laptop or even the Mac PowerBook.

I even tried every TOS emulator I could find, but I never found one that let the personality show through. I can't explain it, but it was like a phantom. It LOOKED like TOS, it FELT like TOS, hell, it even SMELLED like TOS. But it was just an imitation. Even though I copied the ROMs myself (so I know that they were legitimate copies), it was like a cheap gimmick. It just wasn't real.

I guess that's just as well. I've always been of the opinion that, if you're going to use a machine, people like me (those with out either talent or extreme patience) should use native operating systems and applications.

So I've still got a couple of real TOS machines sitting around here, and when I'm feeling the need to actually enjoy using a computer, that's where I go.

Of course, my wife just can't see the reasoning for having these "ancient" computers hanging around, but she's learned to stop asking just before I point to her massive vinyl album collection. <grin>

Well, let's get to the news, hints, tips, and info available from the UseNet:

From the comp.sys.atari.st NewsGroup
==========

Matt Sauer asks about using a PS/2 keyboard on an ST:

"It seems that the QWERTYX box from Becroft is out of production and the maintainer of the Eiffel box is unresponsive. Is there an alternative out there? Does the Eiffel design work? Might another option be to extend the keyboard connecting cable (I guess it looks like some flavor of RJ jack?)? I'm shoving my 520 into a desktop PC case, and I'd like to use a PC keyboard."

Lonny Pursell tells Matt:

"See this page, it looks like Eiffel is still supported.

http://hardware.atari.org/ "

Frederic Pecourt adds:

"Well, there is something I am wondering about : As far as I know, the Eiffel adapter is designed to operate behind one of the historical UARTs of the ST, that is through a serial link. But hadn't someone claimed that UARTs would be DEFINITELY dropped in case that you go for a project of like a G4 based clone with an all-USB approach ?"

Didier Mequignon tells Frederic:

"I think it's easy to modify eiffel and replace classic serial link by and I2C link like the the EEPROM on the SDRAM because today this method is used on the CT60."

Dennis Vermeire tells Matt:

"Peter Denk computers in Germany has manufactured a similar interface, you can connect any PS/2 mouse and keyboard to it, no drivers are needed, a micro-controller emulates the Atari keyboard layout for 100%. It also works with the new batch of wireless devices.

http://www.ATARI-Fachmarkt.de , If I remember correctly, the device is priced at 29 EUR, that's $30 or 20UKP"

Peter West asks a question about file locking:

"There has been a discussion about the lack of file locking on MagiC here. I confess I'm not a programmer, but doesn't the AUTO-folder program CHK_OFLS which comes with Kobold perform this function? It seems to...

On the question of porting GPL apps to MiNT: To my mind, and I suspect the vast majority of Atari users, if these apps run so slowly on 90%+ of existing machines, they are of little interest. To tell people that they need to buy expensive upgrades or new machines to use them is just stupid! They would be better off buying a cheap PC and use that - with or without an Atari emulator."

Lonny Pursell tells Peter:

"No they are not so slow that they are unusable, I have used them on a standard speed Falcon and TT. If you are referring to the text based ones that is, quite usable, as for X11 yeah, you might find that slow."

Peter replies:

"I see, thanks. From the postings in this series it sounded like a CT60 - and there are only 150 of those or the new putative ACP machine was a minimum requirement for usable GPL apps.

I am not anti-MiNT, but for my personal requirements MagiC+NVDI seems extremely stable on my Nemesised 14 MB Falcon and does most of what I want (apart from high-colour graphic-heavy apps such as browsers - and the restriction there is the processor speed, not the OS). Nor do I need multi-user access that would require file locking etc, and I think that goes for the vast majority of Atariites. Those that connect these machines to routers or other computers must be a tiny minority, but I agree that for them the MiNT environment seems to offer advantages. But I'd be surprised if that was more than 1% of Atari users!

But live and let live is my motto - if MiNT suits you, use it."

Well folks, that's it for this week. I know it's short, but it's time to go visit my grandfather again.

Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - SEC Probes Video Game Makers!
  """""""""""""""""""""""""""""""   Fans Mourn 'Doom III' Delay!
                                     Clamor For Console Price Cuts!

=~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""

SEC Probes Video-Game Makers

Four large video game companies have revealed in regulatory filings that they've come under formal investigation by the Securities and Exchange Commission.

Details were scant in the filings by Acclaim Entertainment Inc., Activision Inc., THQ Inc. and Midway Games Inc., but analysts speculated that the SEC probe may be related to an investigation of another game company, Take-Two Interactive.

Take-Two last year restated seven quarters' worth of results over the way it recognized revenue.

Game publishers set aside reserves for a certain percentage of product they ship in case retailers return the product or need to mark it down.

UBS Investment Research analyst Michael Wallace explained in a research note Monday that some distributors have been known to "stuff the channel," or ship product to retailers in order to meet their quarterly revenue expectations, then take the product back from the retailer via excess reserves without affecting the company's income statement.

Wallace noted that most game publishers do business with Take-Two's Jack of All Games U.S. distribution business when they want to move marked-down products.

The SEC notifications for the other game companies could just be fact-finding as an extension of the Take-Two investigation, Wallace said.

He doesn't own shares of any video game company he covers. His firm has had investment banking relationships with Activision, Gamestop Corp. and Midway Games Inc. within the last 12 months, and with Acclaim Entertainment and THQ Inc. within the past three years.

Acclaim Entertainment said it has no comment and will update shareholders as necessary via SEC filings. Officials from Activision and THQ Inc. weren't immediately available for comment.

Shares of all four companies fell on the news.

Eager Video Game Fans Mourn 'Doom III' Delay

There was good news this week for Martian zombies and bad news for the people who love to kill them.

"Doom III," one of the most heavily anticipated PC games ever and a virtual slaughterfest for the interplanetary undead, will not be released this year, the game's publisher said Tuesday.

Buried in video game publisher Activision Inc.'s quarterly conference call on Tuesday was that bad news for hard-core game junkies and others.

A decade ago "Doom" revolutionized PC gaming with its intense graphics. The latest game in the franchise, "Doom III," has been the subject of heavy anticipation ever since creators id Software acknowledged the game was in development.

But when Activision’s president, Ron Doornink, told analysts "for planning purposes, we’re assuming Doom III will come out in the fourth quarter," he shot down those hopes.

Activision’s fourth quarter is the period ending March 2004, meaning the game will not be on shelves for Christmas. As recently as last month, retailers like GameStop Corp. were taking pre-orders expecting a Nov. 15 release.

"I can’t honestly say it’ll be a surprise to anybody," said Rob Smith, editor of PC Gamer magazine. "Basically, the fans out there will sit back and say: ’Yeah, we were expecting that and we’ll hang tight."’

The game’s developer, id Software, is known for its painstaking development efforts. The company’s design guru, John Carmack, is considered a visionary in video game circles whose work has changed the way games look and feel.

At last year’s Electronic Entertainment Expo, a video-only preview of "Doom III" drew legions of fans. The title subsequently won a number of critics’ awards, including "Best of Show."

Games like "Doom III" are so intensive that they play best only on top-of-the-line computers, and some hardware makers have been hopeful that the launch of "Doom" would give them a boost.

Graphics chip designer Nvidia Corp. has been pushing its top processor, the GeForce FX 5900 Ultra, as the best for the new "Doom."

"When we first designed this architecture, we designed it for ’Doom III,"’ Nvidia spokesman Brian Burke said in May.

With "Doom" now off the calendar for this year, a rising competitor looks set to steal its thunder.

At this year’s E3 show, many fans queued up for a preview of "Half-Life 2," also a sequel to a legendary first-person shooter game, from developer Valve. It is scheduled for a September release, according to various retailers’ Web sites.

Clamor Mounts for Video Game Console Price Cuts

If video game publishers agree on one thing it is this: consumers need cheaper platforms in order to start buying more as the $30-billion industry heads toward its make-or-break holiday season.

Three of the largest video game publishers reported quarterly earnings this week, their first since a round of partial game console price cuts in May, and for the most part they said the same thing: not enough, cut more.

That pressure on the three console makers - Sony Corp., Microsoft Corp. and Nintendo Co. Ltd. - amounts to a challenge to accept deeper losses on game hardware in return for profits later as lucrative software sales rise.

That may be a risky strategy but the alternative looks even worse since the most recent data shows sales of the PlayStation 2, Xbox and GameCube down by more than a third compared with last year, a trend that if sustained could make Christmas bleak for hardware and software makers.

In May, most industry observers had expected Sony and Microsoft to cut the prices of their rival PlayStation 2 and Xbox consoles to $149 from $199, and Nintendo to cut the price of its trailing GameCube to $99 from $149, during the industry trade show E3.

Instead, Sony cut the price of the PS2 to $179 and introduced a new version with more features at the old $199 price. Microsoft responded with its own cut to $179. Nintendo stood firm at $149.

Since then, the three have given no indications that they intend to budge from the new prices, despite the calls from their partners in game publishing.

"We continue to anticipate a hardware price cut this fall in order for the console manufacturers to achieve their forecasted hardware sales," THQ Inc. Chief Executive Brian Farrell said on Thursday.

Executives of Activision Inc. said on Tuesday that a price cut was needed.

"In the event there’s no price cut or there’s no promotional equivalent by the holiday season, then we will have to revisit our hardware projections," President Ron Doornink said on a conference call.

Retailers said the cuts by Sony and Microsoft provided almost no boost to sales. That marked a contrast to a year earlier, when Sony and Microsoft took $100 price cuts and Nintendo took a $50 cut and hardware sales boomed.

Even Microsoft conceded last week that the $20 cut on the Xbox had had little effect.

Retailers are starting to speculate that another cut may be in the offing.

"We hear that one, or possibly two manufacturers, are thinking about the price cuts for the fourth quarter. We think the cuts would be good for penetration of the software - new and used," John Antioco, Blockbuster Inc.’s chairman and chief executive officer told Reuters.

Movie rental chain Blockbuster is one of the leading U.S. retailers of video game hardware and software.

But the game industry’s leader, publisher Electronic Arts Inc., said it was not clear yet if console makers were considering a fall price cut or if they would instead choose a strategy, as Nintendo has done, of maintaining the hardware price and bundling in games for free.

"Those are the options available and so far they have not given us a clear indication of which way that’s going to work," Chief Financial Officer Warren Jenson said on a call.

Financial analysts who follow the industry, for their part, think a cut by September to $149 for the Xbox and PS2 and $99 for Game Cube price was increasingly likely.

Those beliefs were reinforced after June sales data from market researchers NPDFunworld showed year-over-year declines in hardware sales of anywhere from 36 percent to 42 percent, due to the tough comparison to last June, when consumers were buying up consoles in a frenzy after the price cuts.

"We believe that the rate of sell-through suggests that a platform price

cut this fall is increasingly likely as the hardware companies try to achieve targeted year-end installed bases," Harris Nesbitt Gerard analyst Edward Williams wrote in a note Monday.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Internet Scams Linked to Identity Theft

Stealing identities and credit card numbers with bogus e-mail and Web sites that appear to come from legitimate companies is an increasing problem on the Internet, federal officials warned Monday.

The Federal Trade Commission said it had brought its first case against this type of scheme, called "spoofing" or "carding." A 17-year-old California boy accused of posing as America Online agreed to settle federal charges by accepting a lifetime ban on sending junk e-mail and paying a $3,500 fine, the FTC said.

The FBI has received increasing numbers of complaints about this kind of scam, said Keith Lourdeau, a section chief with the bureau's Cyber Division.

"Due in part to this growing scam, we are seeing a rise in identity theft, credit card fraud and other Internet frauds," Lourdeau said at a news conference with officials from the FTC and EarthLink. Officials said they didn't know how many people have been victimized by the scam.

In the California case, consumers received authentic-looking e-mails claiming there was a billing problem with their AOL account and asking them to update their information or risk losing Internet access, the FTC said. The message included a link to an "AOL Billing Center," a fake Web page dressed up with the company's logo, colors and links to real AOL sites.

The counterfeit site directed consumers to fix the billing problem by entering credit card numbers and other sensitive personal information including AOL screen names and passwords, Social Security numbers, bank routing numbers, credit limits, mother's maiden name and billing addresses.

AOL spokesman Nicholas Graham said the company will never ask its customers for their password or billing information.

"If they ever get an e-mail purporting to be from AOL that asks them for this information, then clearly it's an online billing scam," he said.

The FTC said the stolen information was used to order merchandise and make online payments worth at least $8,000. The agency said it would not release the name of the teen involved because he is a minor.

"Don't take the bait. Be skeptical of e-mail messages telling you your

account will be shut down," FTC Commissioner Mozelle Thompson said. "If you do receive an e-mail warning like this, don't click on the link."

Instead, he said, people should contact the company directly by phone or through a Web site or e-mail address known to be authentic.

Officials said consumers also should:

_ Be wary of e-mail requests for personal information, especially when they come from companies that should already have the information.

_ Make sure an Internet connection is secure - with an icon of a lock visible on the Web browser - before submitting personal information.

_ Monitor credit card and bank statements for unauthorized charges.

Tips for Internet Users to Avoid Scam

FBI and Federal Trade Commission tips for consumers to avoid Internet scams that use bogus e-mail and Web sites to get personal information:

_Be wary of unsolicited e-mail that asks, either directly or through a Web site, for personal financial or identity information, such as a Social Security number or passwords.

_Don't click on the links provided in such e-mail.

_When updating account information use a familiar process, such as visiting the known Web address of a company's account maintenance page. Unfamiliar addresses for this probably are fake.

_Make sure an Internet connection is secure - with an icon of a lock visible on the Web browser - before submitting personal information.

_Monitor credit card and bank statements for unauthorized charges.

_If an e-mail or Web site is in doubt, make sure the request is authentic by contacting the company directly by phone or through a Web site or e-mail address known to be authentic.

_People victimized by a fraudulent e-mail or Web site should contact their local police department and file a complaint with the FBI and the FTC. Consumers also should report fraudulent or suspicious e-mail to their Internet service provider.

Kinko's Case Highlights Internet Risks

For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.

Jiang had secretly installed, in at least 14 Kinko's stores, software that logs individual keystrokes. He captured more than 450 user names and passwords, using them to access and even open bank accounts online.

The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments.

"Use common sense when using any public terminal," warned Neel Mehta, research engineer at Internet Security Systems Inc. "For most day-to-day stuff like surfing the Web, you're probably all right, but for anything sensitive you should think twice."

Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals remotely access their own computers from elsewhere.

The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around the screen and files open as if by themselves. He then saw an account being opened in his name at an online payment transfer service.

Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as Feb. 14, 2001.

The software is one of several keystroke loggers available for businesses and parents to monitor their employees and children. The government even installed one such program to capture a password that the son of jailed mob boss Nicodemo "Little Nicky" Scarfo used to access files on his computer.

Earlier this year, a former Boston College student pleaded guilty to using similar software on more than 100 computers around campus to collect passwords and other data to create a campus ID card for making purchases and entering buildings illegally, authorities say.

Mehta said that while millions of individuals use public terminals without trouble, they should be cautious.

"When you sit down at an Internet cafe, ask the owner or operator about the security measures in place," he said. "If they don't know or don't have anything in place, you could consider going somewhere else."

Encrypting e-mail and Web sessions does nothing to combat keystroke loggers, which capture data before the scrambling occurs. But encryption can guard against network sniffers - software that can monitor e-mail messages, passwords and other traffic while it is in transit.

Data cookies also contribute to the risk of identity theft. Cookies are files that help Web sites remember who you are so you won't have to keep logging on to a site. But unless you remember to log out, these files could let the next person using the public terminal to surf the Web as you.

Furthermore, browsers typically record recent Web sites visited so users won't have to retype addresses. But such addresses often have usernames and other sensitive information embedded.

Secure public terminals should by default have provisions for automatically flushing cookies and Web addresses when a customer leaves, Internet security experts say.

Kinko's spokeswoman Maggie Thill said the company takes security seriously and believes it has "succeeded in making a similar attack extremely difficult in the future." She would not provide details, saying that to do

so could make systems less secure.

Nonetheless, Thill said customers have a responsibility to "protect their information as they would a credit card slip." She said the company is trying to educate them through signs and other warnings.

At one Kinko’s that authorities said Jiang targeted, a sign attached to individual $18-per-hour stations warns: "BE SAFE. PROTECT YOUR PERSONAL INFORMATION."

Richard M. Smith, a security consultant in Cambridge, Mass., said customers could also use certain techniques to foil keystroke loggers. When typing in sensitive information, for instance, he suggests cutting and pasting individual characters from elsewhere to form the password.

No keys depressed, no characters logged.

ID Thieves ’Phish’ for Victims With Fake E-mails, Web Sites

There’s a new Internet fraud scheme you can add to your list: phishing.

In what the FBI Monday called "the hottest, and most troubling, new scam on the Internet," criminals are sending out millions of fake e-mails to trick online consumers into divulging personal and financial information.

The legitimate-looking e-mails appear to come from some of the Web’s biggest sites, including eBay, PayPal, MSN, Yahoo and America Online, and big-name banks and retailers.

In fact, tech-savvy criminals are collecting the information to commit credit-card fraud, identity theft and even unauthorized bank account transfers from unsuspecting consumers.

The problem has mushroomed this summer, prompting a warning Monday from the Federal Trade Commission and FBI for consumers to beware of criminals fishing for personal identification and financial information.

"Call it ‘phishing,’ carding or brand spoofing, it’s increasing in prevalence," said Eric A. Wenger, an attorney with the FTC who helped prepare the agency’s first law enforcement action targeting the activity.

The phishers spam consumers with bogus requests for a wide range of personal information, ranging from bank account information to credit card numbers to ATM PINs. They direct recipients to phony Web sites that closely resemble legitimate corporate sites.

They hook consumers to give up personal information by claiming billing information needs to be updated or has been lost.

In more brazen versions, the perpetrators actually suggest that the consumer is a victim of fraud and needs to share the information to avoid a fraudulent credit card charge or to prevent more fraud. Other times, the e-mail offers a chance for a prize, a Mercedes-Benz CLK in one case, if a consumer shares personal data.

Some of the culprits are sophisticated Web criminals. But some are just teens.

Take the case of the 17-year-old Los Angeles-area youth who scammed more than $8,000 worth of goods and services, including a laptop and a subscription to online adult-oriented sites. He sent fraudulent e-mails to AOL subscribers, saying there was a problem with their accounts and asking for new credit card numbers. He used that information to set up accounts at eBay-owned PayPal, which he used to make the purchases.

The defendant's AOL look-alike Web page directed consumers to enter the new card numbers. It also asked for mothers' maiden names, social security numbers, bank routing numbers, credit limits, and AOL screen names and passwords. The scheme allowed him to "plunder consumers' credit and debit card accounts and assume their identity online," the FTC said.

The teen has settled with the FTC by paying a $1,400 fine, forfeiting some of the goods and promising never again to send junk e-mail, the agency said.

That case, announced Monday, follows on the heels of a major brand spoofing case last month, when thousands of Best Buy customers received a junk e-mail declaring "Fraud Alert." Citing possible credit card fraud, the e-mails directed consumers to a "special Fraud Department page" supposedly run by Best Buy that asked for the recipients' Social Security and credit card numbers.

News accounts about the phony Best Buy e-mails may have incited more criminals to act, said Linda Foley, co-director of San Diego-based Identity Theft Resource Center.

And in one recent scam, e-mails supposedly from MSN said that technical difficulties arose with July 2003 billing updates. To avoid being terminated, the e-mail urged consumers to enter personal financial information at a "secure online account center." It also offered a bogus customer support phone number, but warned of an average 45-minute hold time on the phone. Microsoft confirmed it was a fraud.

The red flags are not always obvious, said FTC spokeswoman Claudia Bourne Farrell. In the case of the L.A. teen, when consumers clicked on the link, they landed on a site that contained AOL's logo, colors and even links to real AOL Web pages.

If a consumer has even the slightest suspicion, "Do not ever click on those hyperlinks," she said.

While the first reports of "phishing" date back two years, this summer has seen a noticeable uptick.

"We've been bombarded with eBay and PayPal scams" recently, said Foley, seeking "everything about you but your blood type."

Such bogus e-mailing prompted eBay last year to launch spoof@ebay.com, where people can forward suspicious e-mails. EBay said it will never ask for a password online.

EBay spokesman Kevin Pursglove said the company has had about the same volume of complaints over the last six months but acknowledged that e-mail scammers are getting more sophisticated.

"As our anti-fraud tools have more success, they are getting more brazen," he said.

Scamming the Scammers

The e-mail scams, often from the widow of an African dictator, or a bank official, promise untold wealth in return for helping to transfer millions of dollars, but now the "scam-baiters" are hitting back.

They have even succeeded in scamming the scammers: one persuaded his contact to send him five dollars as a sign of good faith; another induced a scammer to send him a sample of the gold dust they were planning to launder - and used it to buy beer for his friends. And one even got a photo of his contact holding up a sign saying "I am a dildo".

They do it with humour - one anti-scammer said his funds would be available as soon as he had sold his shares in the Brooklyn Bridge - but they warn amateurs to be careful.

Victims of the scam have lost tens of thousands of dollars, and in some cases been attacked and robbed. They frequently fail to report their losses to the police - out of shame at their gullibility, and because they had been planning to act illegally.

"This could become a dangerous game, and some of these syndicates can be ruthless," said South African Interpol spokeswoman Mary Martins-Engelbrecht, who added that in South Africa alone some 60 cases of advance fee fraud were reported every day.

The message from the "widow" or the "official" will ask for your name, address, bank details, passport and telephone numbers and a promise that in exchange, you will receive a major cut from the deal.

But first, you will have to pay large amounts of money "to grease palms", for transfer fees, to open a bank account and in many cases, you must travel to the country from where the letter originated.

If you answer, chances are good that you may have just become the latest victim of what is known around the world as the 419 advance fee scam.

Named after a penal code in Nigeria - from where many of the letters originate - the scam works on a simple principle. The victim is being kept on the hook for as long as possible, paying money, with the carrot of a huge return at the end.

The cash never materialises and the scammer disappears into thin air. In some cases, victims are lured into a trap, kidnapped and held hostage for ransom.

Many of the victims are from Europe and Japan, some even from the Caribbean.

"In one of the latest cases, an operation was conducted after we received information that syndicate members lured a female Jamaican attorney to come to South Africa for a fictitious business venture," Senior Superintendent Martins-Engelbrecht told AFP.

"Overall, police here have arrested more than 130 people in connection with the 419 scam," she said.

But now a group of people calling themselves "scam-baiters" are stringing the scammers along at their own game.

One referred a scammer to the west African division of his country - an address that turned out to be the section of Britain’s serious fraud squad dealing with the 419 scams. Another set up a fictitious bank account named "BITROPEY".

"A big part of scam-baiting is the humour but we recognise the seriousness of this fraud. We have to become bigger liars than the scammer to be believed by them," said Neil, a scam-baiter operating out of Australia.

"Some baiters decide to use a theme for one bait, others use made-up pathetic circumstances to tell the scammer, just to show how heartless they are," he said.

He gave an example where a baiter ran an imaginary "home for handicapped children" (the baiter also "confessed" he took regular advantage of the young girls in his care) and where "the roof was in bad need of repair but it would take two years before it could be replaced".

Despite the fact that the baiter told the scammer he only had 12,000 pounds sterling, the scammer persisted with the deal to steal the money from the "children’s home".

But Martins-Engelbrecht warned e-mail users not to enter into any correspondence once a 419 proposition has been received.

"It just gives the criminal more information to work with. Rather alert the police and help us catch the scammer."

And, adds one of the anti-scammers, who asked to remain anonymous: "I would not, considering the fact they are criminals, recommend anybody write to them."

"If someone does feel the urge to do this, exercise extreme caution. Under no circumstances give them your real e-mail, phone number, nor go to meet them."

Field Guide Reveals Spammers’ Tricks

"Mini marquee?" "Lost in Space?" "Hypertextus Interruptus?" Which is your favorite spam technique?

If those names don’t ring a bell, perhaps you should refer to the new Field Guide to Spam, published by enterprise e-mail company ActiveState. The company calls the new online guide a "living compilation" of the tricks that spammers use to slip their unsolicited e-mail messages by antispam filters.

The new guide was conceived by ActiveState Antispam Research Director John Graham-Cumming to quantify spam techniques.

The Field Guide provides a comprehensive listing and explanation of techniques that administrators can use to keep abreast of the ever-changing tricks used by spammers, according to ActiveState. More than 20 different

spam techniques are documented. Each is named and rated for popularity and complexity. ActiveState researchers categorized the techniques as either "common" or "rare," and assigned complexity ratings that range from "dumb" to "dastardly."

In a few minutes, readers can brush up on run-of-the-mill ruses like "Lost in Space," in which the spammer inserts spaces between the letters of common spam "trigger" words such as mortgage and Viagra. Or readers can revel in the subtlety of dastardly techniques like "Slice and Dice," in which a spreadsheet-like HTML table breaks up the content of the spam message, with each cell in the table containing a single letter of the message.

A section on advanced tricks explains how spammers combine multiple techniques in a single message, while also using more technical means for avoiding detection, such as message encoding.

Techniques listed in the Field Guide are used to create heuristic tests that ActiveState's PureMessage e-mail filtering product relies on to spot spam messages, but don't account for all the various types of spam messages, said Jesse Dougherty, director of development at ActiveState.

"These are the techniques used by rogue spammers to hide the content they're sending, usually because it's offensive," he said.

Vancouver-based ActiveState will update the Field Guide whenever new techniques appear and hopes that the catalog helps organizations develop policies to weed out the bothersome messages, Dougherty said.

"Part of industry's challenge is defining spam," Dougherty said. "One test is asking 'Are they trying to trick me?' If an organization cannot verify that a message is not offensive, they can reject it," Dougherty said.

He expects the Field Guide to grow, perhaps to as many as a couple hundred different spam techniques, and hopes that other companies will learn from the guide and contribute to it.

Do-Not-Spam List Finds Favor as Senate Vote Nears

Three out of four Americans favor a "do not spam" registry to keep unwanted e-mail at bay, according to a survey released on Wednesday as the U.S. Senate prepared to vote on the issue before its August break.

The survey of some 1,200 Internet users found broad support for an idea that so far has attracted scant support in the U.S. Congress.

Patterned after the Federal Trade Commission's popular "do not call" registry of households that do not wish to hear from telemarketers, the list would theoretically allow Internet users to make their inboxes off-limits to the online marketers whose unsolicited offers now make up nearly half of all e-mail traffic.

The registry has found an advocate in Democratic Sen. Charles Schumer of New York, who hopes to include a do-not-spam proposal in an anti-spam bill that could come up for a vote in the Senate as soon as this week.

"This survey bolsters the arguments I've been making for a more

comprehensive approach to dealing with spam, including the creation of a no-spam registry," Schumer said.

In testimony before Congress, the FTC has been lukewarm to the idea. Critics say the list would be widely ignored by spammers and would divert resources better spent tracking down those who peddle dubious get-rich-quick schemes.

"We don't think that it's an effective way to spend money that would go toward (anti-spam) enforcement," said Ari Schwartz, associate director of the Center for Democracy and Technology, a nonprofit technology-policy group.

After years of false starts, observers expect Congress to pass some sort of national anti-spam law this year.

On Monday, Senate Majority Leader Bill Frist called spam "a menace." Staffers say the Senate probably will vote on an anti-spam bill before it adjourns for its summer recess next week.

Schumer declined to say whether he would block the existing bill if it did not include the do-not-spam provision.

In the House of Representatives, members of the Energy and Commerce Committee have delayed a vote on the issue until September as they hammer out a compromise between two competing bills.

The survey was conducted July 15 by the ePrivacy Group, a technology company that markets anti-spam products, and the Ponemon Institute, a privacy consulting firm.

Another Anti-Spam Vendor Joins The Fray

Launching an anti-spam software company might seem risky these days. As the spam problem has grown to epidemic proportions, new vendors have been sprouting weekly, and vendors that specialize in other areas, such as E-mail management and antivirus software, have thrown their muscle into the mix. But that's not keeping Eric Hahn, former chief technology officer for Netscape Communications Inc., from joining the fray.

Hahn this week launches his messaging infrastructure venture, Proofpoint Inc., on the basis that too many message-management product categories have developed, forcing customers to purchase too many tools to handle regulatory compliance, archiving, indexing, security, virus protection, and, oh yeah, anti-spam efforts. "The customers are ahead of the vendors here," Hahn says. "They're quick to point out that these stovepipes are out of control."

Still, with its Proofpoint Protection Server, the company is aiming its sights most clearly at spam. Hahn says Proofpoint's combination of machine learning and statistical analysis will trump other anti-spam vendors' offerings by focusing on filtering at both the content and connection levels to counter the constant adaptation of spammer techniques.

For instance, anti-spam filters that scour the content of messages looking for hot-button terminology aren't able to detect tactics such as E-mail spoofing, in which spammers will make a message look like it's coming from

a known E-mail address. "Rules-based vendors are good at detecting what's already known to be spam, but they're terrible at catching spam that's yet to come," he says. "Frankly, customers are more interested in the latter."

Proofpoint is backed by $7 million in first-round venture funding from the likes of Mohr, Davidow Ventures, Benchmark Capital, and Stanford University. The company's pricing - an annual subscription model that starts at $20 per mailbox for a deployment of 500 users - is tailored for huge deployments. There's no charge for the server software, ensuring that customers can count on continuous software updates without needing to budget additional expenditures.

Proofpoint joined two other anti-spam vendors that revealed VC funding Monday. IronPort Systems, founded by former Hotmail exec Scott Weiss, said it had received $15 million, led by Menlo Ventures, and Cloudmark revealed a $4.5 million infusion from Ignition Partners.

The bottom line, Hahn says, is that companies want to get a handle on the spam problem rather than face a never-ending game of catch-up that threatens future use of E-mail. "If we don't stop these guys, we'll be killing the goose that lays the golden egg."

Americans Getting Used To Spam

Although more Americans than ever think that spam should be illegal, a growing number accepts spam as a necessary evil of modern life, according to a Harris Poll released Thursday.

The paradox resulted from a pair of national surveys, one conducted online in May, the other by telephone in June.

The number of people who said that spam was 'very annoying' dropped significantly from last year. In 2003, 64 percent used that phrase to describe spam, a dramatic decline from the 80 percent in 2002.

Likewise, more Americans characterized spam as only 'somewhat annoying' this year than last. In 2003, 29 percent tagged their feelings toward spam that way, a rise from the 16 percent in 2002.

Americans equipped with e-mail receive, on average, 17.2 spam messages, said Harris.

But while consumers may be getting apathetic about spam, that doesn't mean they don't want something done about it.

In the last six months - a time during which Congress has been proposing one anti-spam bill after another - the number of Americans who favor making mass spamming illegal has gone up five percentage points, from 74 percent in December, 2002, to 79 percent in May, 2003.

Just 10 percent of the poll's respondents said they would oppose legislating spam.

Anti-Porn Bill Targets File Sharing

Online file-swapping services would be required to get parental consent before allowing children to use their software under a new bill to be introduced today in Congress.

The Protecting Children from Peer-to-Peer Pornography Act is intended to prevent children from downloading pornographic material, which is widely available for free through file-sharing services like Morpheus and Kazaa.

Besides requiring parental consent, the bill would allow parents to install "beacons" on their computers that signal their desire to not have file-sharing software. If a child tries to download the software, networks would have to refuse when they see the beacon. The beacons would be developed by the Federal Trade Commission with assistance from the Commerce Department.

It also would require file-sharing networks to warn users about the dangers of file sharing. Several studies have shown that the networks are rife with pornography.

There are 57 million Americans who swap files, according to the Boston-based Yankee Group research firm. Forty percent of them are children, according to the bill’s sponsors, Rep. Joe Pitts (R-Pa.) and Chris John (D-La.).

Morpheus, Kazaa and other services have attained notoriety in the past several years for allowing widespread music swapping, but they can be used to trade documents, images, videos and any other kind of digital file. A recent study by Ames, Iowa-based Internet security firm Palisade Systems found that users of the Gnutella file-sharing network searched for pornography more often than they searched for music.

Pitts drafted the bill after reading a General Accounting Office (GAO) study showing the high availability of pornography on file-sharing networks, said spokesman Derek Karchner. GAO investigators in a test of the Kazaa network entered search terms including Pokemon, Britney Spears and Olsen Twins. More than 40 percent of the returns for those searches yielded child pornography, and another 30 percent returned adult pornography.

"He couldn’t sit by and let that happen unregulated," Karchner said.

Fred von Lohmann, a senior staff attorney at the San Francisco-based Electronic Frontier Foundation (EFF), said he is skeptical about the viability of the beacons.

"I’m a little flabbergasted. I have no idea how you would even begin to build such a thing. The reality is that parents have to supervise their kids online and there is no government provision that is going to replace that supervision," he said. "Undergraduate computer science students can write these [file-sharing programs] in under a week. There’s a [mistaken] notion that there might be a company and if there’s a company, federal regulators can grab them."

Wayne Rosso, president of West Indies-based file-sharing network Grokster, said children also can find pornography with popular search engines like Google.

Peer-to-peer "should not just be singled out," he said. "There’s no more or less of a pornography problem on [file-sharing networks] than there is on the entire World Wide Web. Pornography’s only there if you’re searching

for it. It’s not something that just pops up in your face like ’spam’ on AOL."

The GAO study noted that there is far more pornography available on the Internet through normal search engine services than on peer-to-peer networks.

Greg Bildson, the chief technical officer of New York-based file-sharing firm LimeWire, said he has no problem forcing users to confirm that they are adults before downloading LimeWire, but said anything more complicated than a simple question with a yes/no answer would be difficult to administer and could compromise customer privacy.

The Recording Industry Association of America supports the bill, according to a spokeswoman for the group.

The association has sent out hundreds of subpoenas to Internet users suspected of using file-sharing networks to illegally swap copyrighted digital music files.

Tips for Music Fans to Avoid Net Trouble

Tips for music fans to avoid trouble on the Internet:

_It’s almost impossible to check whether you already are targeted for a lawsuit if you have copied music, but some Internet providers are notifying subscribers who are subjects of a subpoena. The San Francisco-based Electronic Frontier Foundation plans to publish - at www.eff.org - information from subpoenas to help computer users determine if they have been targeted.

_If you are targeted, music lawyers may ignore you, send a stern warning or file a civil suit. The recording industry wants to deter downloaders and expects to file several hundred suits in the next eight weeks, but lawyers say they are willing to negotiate settlements.

_The music industry is targeting Internet users sharing "substantial" collections of songs; it has not said how many might qualify for a suit but the minimum number appears to be a few hundred songs.

_Once you download a copyright song, file-sharing software automatically makes it available for other Internet users to download, too. It is possible to reconfigure the software to allow downloads and prevent sharing files, although this undermines the concept of public file-sharing networks.

_The Recording Industry Association of America has said it currently is targeting only Internet users in the United States.

On the Net:

Instructions for reconfiguring file-sharing software:

http://www.musicunited.org/5_takeoff.html

or

http://www.eff.org/IP/P2P/howto-notgetsued.php

Schools Call Music-Use Subpoenas Illegal

Boston College and the Massachusetts Institute of Technology have moved to quash subpoenas seeking the names of students suspected of Internet music piracy, saying they're illegal because they weren't filed properly.

The schools said the subpoenas, issued by the Recording Industry Association of America, didn't allow for adequate time to notify the students, as mandated by the Family Education Rights and Privacy Act.

Boston College spokesman Jack Dunn said Tuesday the school did not object to providing the information.

"We're not trying to protect our students from the consequences of copyright infringement," he said. "Once the subpoenas are properly filed, we will comply with the subpoenas."

Jonathan Lamy, a spokesman for the RIAA, said the association was "disappointed that these universities have chosen to litigate this and thus deny us and other copyright holders the rights so clearly granted by Congress."

Lamy said the association followed federal law when it filed the subpoenas.

This spring, following a challenge by Verizon Communications Inc., a federal judge affirmed the constitutionality of a law allowing music companies to force Internet providers to release the names of suspected music pirates upon subpoena from any federal court clerk's office. Verizon has appealed.

The recording industry association has filed at least 871 subpoenas in U.S. District Court in Washington this month, demanding information from universities and Internet service providers about users of the online file sharing network KaZaA.

It's part of a strategy to jolt Internet music fans to stop file-sharing by pursuing small-time downloaders along with heavier users.

The subpoenas request the names and numbers of one MIT student and three Boston College students who allegedly obtained the music under various screen names.

BC argued in a motion to quash the subpoenas filed Monday that the subpoenas broke federal law because they were served in Boston, more than 100 miles from where they were filed in federal court in Washington D.C.

It also said the subpoenas gave the schools less than a week to produce the information - too little time to properly notify the students under the privacy act.

In a statement, MIT didn't specify why it believed the subpoenas were illegal, but also cited the privacy act to explain why it filed a motion to quash the subpoenas. The school said its decision didn't mean it was taking sides in the debate over downloading music on the Internet for free.

"But we are required by federal law to disclose student information only if we have a valid subpoena and have given the necessary advance notice," Professor James Bruce, Vice President for Information Systems at MIT, said in a statement. An MIT spokesman said the school would have no further comment.

Not all Boston-area schools who've received a subpoena are fighting it. Northeastern University spokesman Rick Mickool said school officials will provide by Wednesday the name of the one student subpoenaed. He said the university's legal counsel had no objection.

Debate Over Zip Format Heats Up

Questions about the splintering of the popular .zip file compression format may soon be resolved by the U.S. Patent Office.

Two months into a was standards battle between WinZip Computing and PKWare over the way .zip software does strong encryption, PKWare, the company that has openly published the .zip specification since it was invented by company founder Phil Katz in 1986, has applied for a patent that it claims will govern the standards in dispute.

"What we've filed a patent for is the whole method of combining .zip and strong encryption to create a secure .zip file," said Steve Crawford, the chief marketing officer at PKWare. The patent was filed with the Patent Office on July 16, he said.

PKWare first added strong encryption to its software in July 2002, including it in the release of its PKZip 5.0 for Windows product, but the company elected not to publish details of how it had done the encryption, claiming that it would be premature to do so before the software had been rolled out on different operating systems like OS/400 and MVS.

"It did not make sense to us to define an implementation... that might subsequently change as we worked through implementation issues on these large platforms," Crawford said.

In May of this year, WinZip developed its own method of strong encryption, which incompatible with the PKWare product. Since then, WinZip and PKWare users have been unable to read each other's encrypted files.

"It's kind of unfortunate," said Darryl Lovato, the chief technology officer with Aladdin Systems, whose company is working on supporting both file formats in its Stuffit compression software. "The good thing about the .zip file format was that you knew you could send it to everyone. Now that's getting broke."

PKWare would clearly like to fix things by having WinZip license its encryption techniques. The company is developing a licensing program for its technique that will be included as part of a "next generation of developer solutions" that PKWare will announce toward the end of this year, according to Crawford.

Crawford believes that WinZip will be a potential licensee. "The basic approach of combining encryption of .zip is covered by the patent, so what WinZip has done, I believe, would be covered by the patent."

Of course, PKWare will first have to be issued a patent by the U.S. Patent Office before it can begin charging licensing fees, and this may not prove easy, according to Lovato. "Encryption and archives have been around for a very long time and there's prior art all over the place," he said.

Lovato said that, should PKWare be awarded a patent, his company would consider paying a licensing fee, depending on its cost. "If they want $10 a copy for every unit we sell, there's no way we'd do that," he said.

Crawford did not know when the Patent Office would rule on the application. The process could take years, he said.

WinZip could not be reached for comment on the matter, but IDC analyst Charles Kolodgy did not expect a positive reaction to the news from the largest provider of .zip compression software. "Given WinZip's position on the desktop, they probably would not feel to good about it," he said.

Should PKWare be awarded a patent, WinZip may simply decide not to include strong cryptography in their product and avoid any licensing fees, since strong encryption is not an important feature to the majority of desktop users, he said.

Lovato did not think that adding a licensing fee to the 17-year-old free standard would be good for .zip, which, he said, has beginning to show its age. "It's certainly not going to help it remain the standard for longer," he said. "I think it's just another nail in the coffin."

Online Voting Moves Closer To Reality

Americans living abroad, including thousands of military personnel, may get a chance to vote in the 2004 election from any Windows-based computer linked to the Internet. The Defense Department's Federal Voting Assistance Program, known as FVAP, is working with 10 states to develop the Web-based voting system called Serve-Secure Electronic Registration and Voting Experiment.

County election officials in participating states will use Serve to receive voter-registration applications, provide ballots to voters, and accept ballots when they're completed. Existing election-administration systems will be used to process registration and ballots.

In a statement issued by FVAP, director Polli Brunelli says security is everyone's first question about Internet voting, adding that the government made security the driving factor in Serve's system design.

States expected to participate in Serve are Arkansas, Florida, Hawaii, Minnesota, North Carolina, Ohio, Pennsylvania, South Carolina, Utah, and Washington.

According to FVAP, the government successfully conducted a small-scale proof-of-concept pilot, Voting Over the Internet, for the 2000 election. In that experiment, 84 citizens in 21 states and 11 countries returned ballots to jurisdictions in Florida, South Carolina, Texas, and Utah, the first time citizens cast binding votes over the Internet for government offices.

Eligible U.S. citizens can register to use Serve in 2004 by accessing its Web site, www.serveusa.gov.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.